On Cyber Security of Industrial Measurement and Control Systems

Stevan Milinković
Union University, School of Computing
Belgrade, Serbia
smilinkovic@raf.edu.rs

Ljubomir Lazić
State University of Novi Pazar
Novi Pazar, Serbia
llazic@np.ac.rs

***Abstract* – Modern industry wouldn't exist without sophisticated computer-based measurement and control systems. This paper shows that industry measurement and control devices have the same sorts of vulnerabilities and exploits as general purpose computers and networks. However, the consequences of production interruption due to measurement or control system failures are much more serious than failures within the business network. The industry dedicates huge time and resources toward ensuring the safety of its personnel, customers, and surrounding community. But in today's environment of growing cyber threats, an industrial plant is not safe unless its systems are secure.**

Key words – system safety; plant security; cyber security; industrial control systems

I. INTRODUCTION

Information technology is the backbone of nearly every aspect of today's modern society. Reliable information technology is key to engineering new scientific developments, managing the supply chain, executing processes in plants, maintaining productivity in offices, storing employee benefit and payroll information and securing business and manufacturing control systems. As technology continues to advance, so will the industry's use of IT to improve the way it conducts business. Applications include, but are not limited to modeling, numerical analysis and simulation, optimization, process and product synthesis and design process dynamics, control and monitoring, abnormal events management and process safety, plant operations, integration, planning, scheduling and supply chain, enterprise-wide management and technology-driven policy making, domain applications (molecular, biological, pharmaceutical, food, energy, and environmental systems engineering) etc. Willing or not, we all live in a digital age. The proliferation of digital technology, and the convergence of computing and communication devices has transformed the way in which we socialize and do business. While overwhelmingly positive, there has also been a dark side to these developments. So we come up to cyber security - protection of information technology systems and networks, as well as the programs and information within them from hostile actions. And there, things are not so good.

A report from Cisco [1] indicates as in 2013, among the top 10 pharmaceutical and chemical industries were at the highest risk of malware attacks by cybercrime. The annual cybercrime global survey carried out from the Ponemon Institute [2] illustrates that cybercrime costs economies billions annually, with pharmaceutical, chemical and petrochemical companies among the hardest hit.

Perhaps the greatest threat today is the abysmal state of security of so many of the systems connected to the Internet. There are many contributing factors, including commercial off-the-shelf software, in which the number of features and rapid time to market outweigh a thoughtful security design. The widespread use of many such products means that once a vulnerability is discovered, it can be exploited by attackers who target many of the thousands or even millions of systems that have the vulnerable product installed [3].

II. INTEGRATING INDUSTRIAL AND CORPORATE IT

A new industrial revolution is taking place on the factory floor as corporations discover the economic benefits of integrating their Information Technology (IT) networks with legacy process measurement, control and production systems. In addition, the new gadgets and smaller, better, faster computers have been developed with revolutionary speed. But while the IT and computer-based markets evolve rapidly, the industrial side of the end-user market is fairly slow to adapt. It is sometimes considered too expensive to do so, or too disruptive to the process or production.

Capital equipment is intended for long-term use, and is likely to remain in use for 10-20 years, until the capital expenditure has been amortized. As a result, it is not uncommon to find that the processors used in the equipment controls may be older versions, as well as older versions of operating systems. These reduced performance processors have long been obsolete, and there is a lack of support for upgrades or software-based security solutions for obsolete technology. Even more critical are the security risks for older Windows operating systems such as Windows 98, because Microsoft no longer supports these versions with security updates.

It should be noted that support for Windows 2000 has expired in July 2010. Microsoft announced the end of support date for Windows XP SP3: 8 April 2014. Security issues with Windows Vista, 7 and 8 are currently being reported with considerable frequency. Similar problems exist for PCs running on the operating systems from other manufacturers. Often, older versions are no longer supported and security holes can no longer be closed through software patches. And some processes or production lines cannot easily be interrupted to install frequent patches or software upgrades. An upgrade must

Results are part of the research that is supported by Ministry of Education and Science of the Republic of Serbia, Grants No. III-45003 and TR-35026.

be tested and proven to do no harm before incorporated into a production line.

On the other hand, traditional systems used in the corporate network have the drawback that they can always be identified based on their Internet Protocol (IP) address – and are therefore highly susceptible to attack. This is particularly due to the fact that in many systems, specific numbered ports are left open in order to ensure unproblematic data transfer via the Internet connection.

In the mean time, industrial users found significant cost reductions and huge productivity gains in selective installation of a LAN network technology. Ethernet, an open standard and an already established connectivity technology on most business networks, would find similar value as control and system engineers began to thread together various 'islands-of-automation' into a plant-wide control network infrastructure. Soon most industrial devices were designed to be "Ethernet-enabled". Ethernet became ubiquitous and the Internet more pervasive as IP technology connected everything for an anywhere, anytime, access-to-data experience. Industrial wireless sensor technology with its self-configuring, self-healing mesh approach further added to the networking infrastructure. PLCs are beginning to connect beyond the confines of the factory floor, e.g. via iPhone applications that display status data or even control PLCs directly via over-the-air commands [4].

In addition, it is common practice today to include access to web-based services on most PLCs. According to a major manufacturer of PLCs, the majority of their products are ordered with web services enabled. Yet their own study indicated that only 13% of customers actually configured and used the web services. So 87% of users left the web servers in the PLCs with factory default passwords, like "1234" [5].

III. SCADA

Supervisory Control and Data Acquisition (SCADA) systems have evolved over the past 40 years, from standalone, compartmentalized operations into networked architectures that communicate across large distances. In addition, their implementations have migrated from custom hardware and software to standard hardware and software platforms. These changes have led to reduced development, operational, and maintenance costs as well as providing executive management with real-time information that can be used to support planning, supervision, and decision making. These benefits, however, come with a cost. The once semi-isolated industrial control systems (ICS) using proprietary hardware and software are now vulnerable to intrusions through external networks, including the Internet, as well as from internal personnel. These attacks take advantage of vulnerabilities in standard platforms, such as Windows, and PCs that have been adopted for use in SCADA systems [6].

The control components of SCADA systems are optimized to provide deterministic, real-time performance at a reasonable cost. Thus, there are little computing resources available for executing other functions not considered necessary for the basic SCADA mission. As a result, SCADA system manufacturers view additional computing tasks, including information system security, as burdens on the computing capacity that could interfere with the proper operation of the system. Information system security was not inherent in SCADA protocols because, when the protocols were developed, SCADA systems were usually operating in closed environments with no vulnerable connections to the outside world. In today's SCADA applications, the opposite is true. SCADA systems are connected to corporate IT networks and use protocols and computing platforms that are under attack in the conventional IT world.

SCADA system based cyber security attacks have the very real possibility of impacting life safety, the environment and organizational survival. In a worst case scenario, say a SCADA system cyber attack successfully penetrates a refinery system. In this scenario, the attacker alters some critical data to reflect a safe condition while blocking the ability to generate essential safety control commands. In this situation, the process could easily exceed a safe limit, an explosion and fire could occur which not only costs the loss of life but also destroys the firms basic process infrastructure. The refinery could go out of business. From this example it could be easily seen that SCADA system cyber security attacks can have a much greater impact on the organization than an IT cyber security attack.

Another reason IT cyber security processes cannot be directly applied to the SCADA system is associated with how the systems must operate, i.e. system availability. SCADA systems must operate non-stop where system outages and interruptions are not tolerated. This is a different environment than IT systems where planned system outages or unavailable times can be planned and do occur. A prime example of how the different availability technology requirements impact cyber security approach is highlighted with operating system updates.

Most, if not all, computer operating systems vendors routinely transmit or notify the end user that software updates are available for their system. These updates may address newly identified cyber security issues or software bugs. For single system owners, implementing an update maybe as simple as agreeing to the update and the operating system performs all functions. For other organizations the IT department may have update policies and procedures that define how updates are implemented and how the system will be returned to a known, good state in case an issue with the update occurs.

As an example, an IT group may require that all operating system updates occur between the hours of midnight and 3 a.m. This time frame is selected as most people are not on their computer during those hours. The time also allows the IT group sufficient time to restore the system to a pre-update state if a problem develops during the changes. While the intent of the operating system update policies and procedures is to minimize end user impact, it does not state that the system will not be in service at all times. In fact, very often a part or most of the entire network is not in service during major operating system modifications. Acknowledging and accepting that enterprise systems or applications may experience outages, for some period of time, is often a normal organizational operating state.

With SCADA systems it is not business as usual if the system is not operating non-stop. The control room operator

cannot monitor and control critical field processes if the SCADA system is not in service. The need to have the SCADA system always in operation requires a different system update and modification policy and procedure than what and how the enterprise system performs its updates.

Another area where IT cyber security practices are not directly transferrable to the SCADA world is in the area of intrusion detection and prevention systems (IDPS). Within the enterprise IT domain, the use of an IDPS is fairly common and adds another layer of cyber security. Yet, as stated above, SCADA systems sometimes utilize unique protocols which are not supported by today's IDPSs and the available IDPSs rule sets are not fully applicable to the SCADA environment. As this technology matures, its acceptance within the SCADA domain will probably increase. In the interim, directly applying an enterprise IT based IDPS within the SCADA system may generate issues rather than enhance cyber security.

Network monitoring is another distinct domain difference that has not matured to a degree that the IT based systems can be easily applied to the SCADA network. This is a different landscape than the IT enterprise system which has a suite of various network monitoring systems that can be and are deployed.

SCADA systems cyber security challenges are also slightly different than enterprise systems in the areas of vendor certifications, anti-virus software verifications and password rules as well. Vendor supplied SCADA applications function within the operating system. The vendors provide extensive testing and validation that their SCADA system will perform as designed with a specific computer operating system. This is very much the same as many enterprise software applications. The difference comes about in how fast, if ever, that the software vendor provides certification that its SCADA system will operate correctly with the latest set of updates or the next operating system version. It is not uncommon to find some SCADA vendors are extremely slow in providing validation or that they will never validate that their older systems are capable of operating correctly with a newly released operating system.

SCADA vendor validation that their systems correctly work with most anti-virus software is an area that is lacking across many vendor systems. While the enterprise IT department deploys anti-virus software and updates the virus signature files on a routine basis, SCADA systems often cannot follow this same process. This limitation is directly tied to the SCADA software vendor's ability to verify that their system will correctly operate with the anti-virus software and all the new virus definitions that are supplied. SCADA vendors are smaller organizations that lack sufficient staff resources to keep up with this rapidly advancing field. Due to vendor resource constraints, SCADA system end users are often faced with the internal decision to self verify that their network will work with anti-virus software or to give up utilizing these applications.

Several operating system patching update approaches are present within the SCADA discipline. Some firms take the position that they will not update their SCADA operating system unless required by the SCADA vendor. In this situation, the SCADA computer operating system falls further and further behind the original vendor supplied system.

A second approach is that on a planned schedule all updates are first tested on an offline SCADA system. If the testing indicates that the updates will not adversely affect the network, these changes are loaded into one computer at a time and system normal operation is verified prior to implementing the changes on any other site.

A third approach is a slight modification of the second approach. This approach still validates that the operating software updates will not affect the offline system. Once this is validated, the operating system updates are loaded into the backup, offline, SCADA system. The backup system is monitored for some time to ensure no adverse impacts are noted. Once a level of confidence is obtained, the backup system is transitioned to prime and operation is closely monitored.

It is reasonable to assume that if we are updating our Windows computers on our SCADA system (using some variation of Microsoft Windows Update), then any vulnerable services that can be patched will be patched. Unfortunately that is not true – we may still have a number of open vulnerabilities that are being missed by the Windows update service. And we can't do much about it, as explained in [6].

To understand why this is possible, it helps to know a little about something called Windows Common Controls. Common Controls are executable routines that Microsoft supplies to give applications from different developers for a unified look and feel. For example, the Tool Tip Control creates those small rectangular windows that display help text when we place the cursor over some button or tab and wait for a while.

Common Controls have been in use from the early days of Windows. Applications like Word or SQL Server use them extensively, but so do many developers of 3rd party applications. In the SCADA and ICS world, it is a fair guess that the bulk of the software developed for industrial server or client applications on Windows machines use them.

The problem started when Microsoft announced the existence of two serious vulnerabilities [8, 9] in the ActiveX controls contained in the file MSCOMCTL.OCX. According to the CVE database [10], these flaws were being exploited as targeted attacks in April 2012 using specially crafted malicious RTF files sent via e-mail. Microsoft soon provided patches to fix these vulnerabilities in their April and August 2012 patch releases.

However, it seems that the Windows Update service will deliver the patches only when qualifying Microsoft products, such as MS Office, are detected. If our computer isn't running an application like MS Office, Microsoft SQL Server or Microsoft BizTalk Server, it won't get patched. It doesn't matter if our computer has a critical SCADA application that uses the vulnerable OCX file, we are out of luck.

To make matters worse, even standalone updates from Microsoft fail during installation unless the qualifying Microsoft product is detected. And tools like Microsoft Baseline Security Analyzer (MBSA) will miss this as well, because as soon as MSBA sees that we don't have the qualifying application (e.g. MS Office) installed, it doesn't bother to check if the MSCOMCTL.OCX file is current.

It is important to know that these Windows Common Controls were extensively used in many SCADA and ICS products. Yet very few computers in industrial automation settings run applications like Microsoft Office. A few running Microsoft SQL Server will get patched, but 99% of the SCADA and ICS computers will not get this critical patch. According to [9], Independent Software Vendors that have products using the Windows Common Controls should repackage their product with the latest updates. But how many ICS vendors will do that? And how many control system users will install that update in a timely manner? This likely won't be an automatic update of a single file – it could be a new package to install. And, even if the patch is available, it needs to be tested and certified. The SCADA/ICS world is facing a situation where there will be a massive number of unpatched and vulnerable computers running on critical systems for the next years. And that is not good news.

This is an example of how the entire strategy of patching for SCADA and ICS security is broken. Vendors are reluctant to supply patches for many control products (especially legacy products), and users are reluctant to deploy patches when they get them. Furthermore, even when we think we are patching our system, we might not be. That is why the European Coordination Action to foster progress towards cyber security of industrial control systems is started in the first place [11].

IV. PLC

Introduced in the late 1960s, Programmable Logic Controllers (PLCs) were designed to eliminate the higher cost of complicated, relay-based control systems. By the 1980s, Distributed Control Systems (DCS) achieved popularity within increasingly automated plant environments, with keyboards and workstations replacing large, individual control cabinets. Entire production lines and processes could be linked over industrial cable/bus networks (Modbus, Profibus, Fieldbus and others) to provide monitoring and control to a foreman's desk. Dials, gauges and indicator lights were replaced by a pictorial representation of the process with fields displaying real-time information. The available systems were in every sense proprietary, capturing market share by staying incompatible with competitive systems. In the early 80's a strategy to decentralize proprietary process control systems emerged and spawned the Fieldbus wars. Thus began the unraveling of central control strategies with a vision towards driving more intelligence into each field device and utilizing non-proprietary technology.

Today, almost every PLC, DCS, Remote Terminal Unit, or Safety Integrated System (SIS) controller on the market has a commercial operating system in it. Microsoft Windows vulnerabilities are abound and reported in various resources on the Internet. Similar is with Linux and QNX.

As for OS-9 and VxWorks, these operating systems are not famous like Windows or Linux, and consequently their bugs and vulnerabilities are less known. However, vulnerabilities are still there, and here are some examples.

Microware OS-9 [12] is a multi-user, multi-tasking UNIX-like operating system. It has been shown to be susceptible to attacks using ICMP redirects. An attacker could forge ICMP redirect packets and possibly alter the host routing tables and subvert security by causing traffic to flow on a path the network manager didn't intend.

VxWorks (product of Wind River Systems, acquired by Intel in 2009) is more famous embedded real-time operating system. It has been used to power everything from the Apple Airport Extreme access points and BMW iDrive to the Mars rovers and the C-130 Hercules aircraft. Unfortunately, it has two serious flaws, described in [13, 14].

The first flaw refers to an exposed VxWorks debug service (WDB Agent). This service runs over UDP port 17185 and allows complete access to the device, including the ability to manipulate memory, steal data, and ultimately hijack the entire operating system. This service was inadvertently left exposed by over 100 different vendors and affects at least 250000 devices sitting on the Internet today.

The second flaw relates to a weak password hashing implementation in the VxWorks operating system. Any device that uses the built-in authentication library to handle Telnet and FTP authentication can be compromised. The flaw occurs because there are only 210000 possible hash outputs for all possible passwords. An attacker can simply cycle through the most common ranges of hash outputs of about 8000 work-alike passwords to gain access to a VxWorks device. Using the FTP protocol, this attack would only take about 30 minutes to try all common password permutations.

Schneider Modicon devices are the stories of their own. It can be easily seen directly from Schneider's firmware that there are a huge number of hard-coded accounts in the devices [14]. These accounts let a user do anything to the device, i.e. they all have the same privileges. For example, you can upload a new firmware to the device and use the Ethernet module in a Modicon as a general-purpose computer. Even you can run Linux on it. Schneider left debugging symbols in the firmware, which are pretty easy to reverse engineer. Some of documented Schneider Modicon vulnerabilities are reported in [15, 16].

A. Case study

The Allen Bradley Logix family is the most full featured programmable controllers in the line of Rockwell Automation. The ControlLogix is the flagship product of the Logix family. It consists of a chassis with controller, power supply and I/O modules that can be used as both a controller and a gateway. The number and type of modules is determined based on the size and type of system being controlled, network topologies and protocols, and redundancy requirements. Its configurations can vary greatly with the large number of modules and ability to mix and match to meet requirements. The 1756-ENBT and 1756-EWEB (with web server) modules provide an Ethernet connection to the ControlLogix and warrant special attention from an information security perspective.

A wide range of control system protocols are supported on the ControlLogix platform. For communication from a server, HMI or other controllers, the ControlLogix supports EtherNet/IP, ControlNet and Data Highway as well as other standard protocols from third party modules such as Modbus TCP. Protocol support for I/O communication includes the

EtherNet/IP, ControlNet and DeviceNet plus HART, Foundation Fieldbus and other standard protocols. Since this is a popular controller platform, there is a good chance that most control system protocols are supported directly by Rockwell Automation or by a third party product that can be integrated in the ControlLogix platform.

As more capabilities are pushed out to the device like the ControlLogix, they become a more crucial component in a control system and a bigger target. One of the simplest means to secure a ControlLogix is to physically place the controller modules into Run mode and remove the physical key. Unfortunately this prevents remote management and viewing of the configuration. This may be acceptable in small DCS but would be place a burden and delay response in a geographically dispersed system.

B. *Exposed services*

1756-ENBT/A brings Ethernet connectivity to the controller, thus opening up the door to a whole range of remote attack vectors. For example, it could be easily seen via nmap:

```
snmp-netstat:
TCP 0.0.0.0:80     0.0.0.0 ; http (GoAhead)
TCP 0.0.0.0:111    0.0.0.0 ; rpcbind
TCP0.0.0.0:44818   0.0.0.0 ; EtherNet/IP
UDP 0.0.0.0:68     *:*     ; dhcp(if enabled)
UDP 0.0.0.0:111    *:*     ; rpcbind
UDP 0.0.0.0:161    *:*     ; snmp
UDP 0.0.0.0:2222   *:*     ; EtherNet/IP
UDP 0.0.0.0:44818  *:*     ; EtherNet/IP
```

Port 44818 is used by the Rockwell Automation software (RSLogix, RSLink…) drivers to communicate with those ControlLogix controllers which have EtherNet/IP modules enabled.

EtherNet/IP is an application layer protocol treating devices on the network as a series of "objects". It is built on the Common Industrial Protocol (CIP), for access to objects from ControlNet and DeviceNet networks.

RSLogix, RSLinks and other Rockwell Software can be easily downloaded from Rockwell's support website. By interacting with this software while monitoring the network traffic we can easily analyze and extract the packets needed to monitor and control the PLC i.e. obtain information about the processes running on the CPU or update the firmware.

C. *Live system*

With the little help from Shodan search engine [17] it is easy to find ControlLogix devices on the web. The first site we have found was www.scrapmetal.net (American Iron & Metal Co. Inc.). We get there immediately when we enter http://204.101.14.75/index.html in our browser. It is an 1756-ENBT/A web page with completely operational menu on the left side, including the full diagnostics and refreshing rate every 15 seconds. It could be easily seen that the firmware date is Jan, 7 2005. This is valuable information for someone who wants to prepare an attack to the device. ControlLogix uses GoAhead web server, which is a simple, portable and compact web server for embedded devices and applications. It is one of the most widely deployed web servers and is embedded in hundreds of thousands of devices. Unfortunately, this web server contains vulnerabilities that may allow an attacker to view source files containing sensitive information or bypass authentication. The information disclosure vulnerability was published in [18].

D. *Configuration*

All configuration of the ControlLogix controller is done over via EtherNet/IP, for example using RSLogix desktop software. Authentication is optional which means that brute-forcing is possible, because there are no timeouts/lockouts. Moreover, lots of functions don't require authentication so the following attacks can be performed [19]: change the IP, forcing a CPU stop, crash CPU, dump 1756- ENBT's module boot code, reset module, crash 1756-ENBT module, and flash update.

V. SMART METERING

The evolution of wireless technologies has allowed industrial automation and control systems to become strategic assets for companies that rely on processing plants and facilities in industries such as energy production, oil, gas, water, utilities, refining, and petrochemical distribution and processing. Effective wireless sensor networks have enabled these companies to reduce implementation, maintenance, and equipment costs and enhance personal safety by enabling new topologies for remote monitoring and administration in hazardous locations. However, the manner in which sensor networks handle and control cryptographic keys is very different from the way in which they are handled in traditional business networks. Sensor networks involve large numbers of sensor nodes with limited hardware capabilities, so the distribution and revocation of keys is not a trivial task.

According to [20] an untrusted user or group within a 40-mile range could read from and inject data into these devices using radio frequency transceivers. A remotely and wirelessly exploitable memory corruption bug could disable all the sensor nodes and forever shut down an entire facility. When sensors and transmitters are attacked, remote sensor measurements on which critical decisions are made can be modified. This can lead to unexpected, harmful, and dangerous consequences.

VI. SAFETY IS NOT SECURITY

Security, safety and compliance are not the same. We can be secure but not compliant, and vice versa, we can be compliant but not secure.

While functional safety addresses the negative impact (i.e. the damage) procured by a plant/equipment on the surrounding environment, security addresses primarily the damages that the surrounding environment may cause to the plant [21]. The likely impact of being unable to view or control the process or system is an increased reliance on emergency and safety systems. Traditionally these systems have been totally independent of the main control systems. However, mirroring the trend in the design of the main control systems, these emergency systems are also becoming based on standard IT technologies. They are increasingly being connected to or

combined with the main control system, increasing the potential risk of common mode failure of both the main control system and the safety systems. Consequently, the systemic risks of cyber attack need to be considered in the design of not just the control systems, but also the safety systems.

So far the priorities for design requirements for control systems consisted of performance, reliability, and safety — not security. Security is not only a new constraint, but also often goes in the opposite direction of reliability and safety. Securing a system requires retrofitting new security requirements where none previously existed. Traditional security strategies, such as changing default passwords, don't necessarily work in a control system environment. In fact, changing the default passwords in a PLC could effectively shut down the PLC. That's not to say operators shouldn't take advantage of the security measures that come with the Windows human machine interface component of the industrial control system. However, security is more difficult as we move into the hardware component of control systems, such as PLCs, analyzers, variable-frequency drives, and smart transmitters.

VII. CONCLUSION

With the modernization of control system equipment more systems are interconnected and more importantly, more systems are linked at some level to the Internet. With each additional connection comes one more doorway by which a hacker, curious or malicious, can enter.

In the world of industrial systems where efficiency is critical to making a profit, an undetected cyber attack can slow the process and reduce the efficiency of the plant. Clearly, companies that do not pay adequate attention to their cyber security are at risk and implications of cybercrime within the particular industry go beyond the obvious financial damage. Cybercrime also sparks off legal implications through customer and client lawsuits, loss of productivity due to crimeware infections and subsequent downtime, as well as personal accountability for company executives held directly responsible for data breaches. This can lead to brand damage, since once organizations are exposed in the media for breaching data, it can be difficult to recover public trust.

Until recently, few people knew about PLC vulnerabilities and attack tools. This all changed when Stuxnet came out – now every hacker in the world knows about PLCs, SCADAs and the opportunities to attack them. Worst still, it showed the world that finding a zero-day vulnerability isn't even required to attack most PLCs – you just need to get a foothold in a computer that communicates to a PLC. It is time to start protecting the industrial controllers. There is no silver bullet, but it is believed that shielding them with firewalls and VPNs from all other equipment on the network is an important start.

Recent wireless communication technologies have enabled the creation of new plant automation architectures that give organizations strategic advantages by replacing key pieces of their hard-wired infrastructure. These advantages include cost savings in logistics, installation, and engineering, as well as better data acquisition frequency and reliability. These wireless solutions also provide remote and localized control, allow for the efficient transmission of current and historical data to an organization's central office, and reduce the need to physically access potentially dangerous systems and machinery.

These devices may pose security threats for some time to come. However, researchers are continuing to write academic papers about the future of wireless sensor networks and key distribution. Using out-of-bands methods to pre-share a strong secret for the initial link is a desired practice as well as enabling encryption features at every layer possible of the protocols used. Securing the node physical access is recommended maximizing the protection over the trust center.

REFERENCES

[1] Cisco Annual Security Report, Cisco Systems, Inc., 2014.

[2] Research Report, *2013 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, 2013.

[3] H.F. Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMU/SEI-2002-SR-009, Carnegie Mellon University, 2002.

[4] ScadaMobile User Manual, Version 2.1.8, SweetWilliam, S.L. Llevant, 10 17844 - Cornellà del Terri, Spain.

[5] R. J. Turk, Cyber Incidents Involving Control Systems, US-CERT Control Systems Security Center, Idaho Falls, 2005.

[6] R.L. Krutz, Securing SCADA Systems, Wiley, Hoboken, 2006.

[7] E. Byres, The Critical SCADA Security Patch that your Control System Isn't Getting, Tofino Security, October 12, 2012.

[8] Microsoft Security Bulletin MS12-027 – Critical Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258) – updated April 26, 2012.

[9] Microsoft Security Bulletin MS12-060 – Critical Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573) – updated August 22, 2012.

[10] CVE. A dictionary of publicly known information security vulnerabilities and exposures, 2012. Available http://cve.mitre.org/ .

[11] I.N. Fovino, A. Coletta, M. Masera, Taxonomy of security solutions for the SCADA sector, ESCORTS Deliverable D22, Security Technology Assessment (STA) Unit - Security of Critical Networked Infrastructures (SCNI) Action, Joint Research Centre of the European Commission, Version 1.1, 09 March 2010.

[12] J. Russell, R. Cohn, OS-9, Bookvika Publishing, 2012.

[13] US-CERT Vulnerability Note #362332: Wind River Systems VxWorks debug service enabled by default, 23 July 2012.

[14] US-CERT Vulnerability Note #840249: Wind River Systems VxWorks weak default hashing algorithm in standard authentication API (loginLib), May 10, 2012.

[15] ICS-ALERT-11-346-01 – Schneider Electric Quantum Ethernet Module Multiple Vulnerabilities, December 12, 2011.

[16] ICS-ALERT-12-020-03 – Schneider Electric Modicon Quantum Multiple Vulnerabilities, January 20, 2012.

[17] Eric Byres, "Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting", *Tofino Security*, 2013.

[18] US-CERT Vulnerability Note #975041: GoAhead Web Server discloses source code of ASP files via crafted URL, 11 Jan 2010.

[19] R. Santamarta, Attacking Controllogix, Digital Bond Project Basecamp, 2012. Available: http://www.reversemode.com/

[20] Lucas Apa, Carlos Mario Penagos Hollman, "Compromising Industrial Facilities from 40 Miles Away", *IOActive Technical White Paper*, 2013.

[21] E. Ciapessoni, R.Cortina, La sicurezza funzionale nel sistema elettrico di potenza:stato della normativa tecnica applicabile, Gennaio Febbraio 2006 – 1 Rivista AEIT, "Sicurezza dei Sistemi".